Department of the Army
266th Finance Command
Unit 29001
APO, AE 09007

Computer-User Agreement

APPENDIX A
COMPUTER-USER AGREEMENT
This agreement is also available on the USAREUR Automation Training Program website at **https://www.uatp.hqusareur.army.mil**. Your information management officer (IMO), system administrator (SA), or information assurance security officer (IASO) will ask you to sign a copy of this agreement before issuing you login credentials (user-ID and password). As a user of information systems in the Army in Europe, I will adhere to the security requirements outlined in DOD, Army, and Army in Europe policy, in particular the information assurance (IA) policy described in AE Pamphlet 25-25, with special attention directed to the following:

1. I will use Army information systems (computers, systems, and networks), operating systems, and programs only when authorized and only for authorized purposes.

2. I understand that my use of Government communications systems and networks serves as consent to authorized auditing and monitoring.

3. I will not install software or install or move hardware on any Government computer (GC) or network without the written approval from my IMO, SA, IASO, or (in the case of major changes) my designated approving authority.

4. I understand that the use of employee-owned information systems or devices on an Army in Europe network is prohibited, as is the processing, storage, or transmission of sensitive official information on such systems.

5. I know I will be issued a user-ID and password to authenticate my computer account. After receiving them—

a. I am responsible for all activity that occurs on my individual account. If I am a member of an authorized group account, I am responsible for all activity when I am logged onto a system with that account.

b. I will not allow anyone else to have or use my password. If I suspect that my password is compromised, I will report this immediately to my SA.

c. I will not forward chain e-mail (example: rewards from various companies by simply forwarding an e-mail message). I will report chain e-mail, or virus warnings to my IAO and delete the message.

d. I will ensure my password meets length and complexity requirements by comprising a total of at least 10 characters, with at least 2 lowercased letters, 2 uppercased letters, 2 numbers, and 2 special characters.

e. I will ensure that my NIPRNET and (if applicable) SIPRNET passwords are changed at least once every 90 days and changed immediately if compromised.

f. If my account is on a classified network, I understand that my password is classified at the highest level of information on that network, and I will protect it accordingly.

6. I will ensure that the antivirus software on my GC is updated at least weekly, and I will scan all e-mail attachments, other media, and other devices for malicious code before opening attachments or using the devices on a GC or on an Army in Europe network.

7. I will not use Internet "chat" services (for example, America Online (AOL), Microsoft Network (MSN) Instant Messenger, Yahoo) from my GC. If a chat service is required, I will use my AKO account.

8. I know that if connected to the SIPRNET, my system operates in the U.S. or NATO (as applicable) Secret "system-high" mode.

a. I will not enter information into a system if the information has a higher classification than that for which the system and network are accredited. If the information is proprietary or requires other special protection, I will seek guidance from my IASO.

b. I will protect all data and output at the system-high level unless or until the information is downgraded or declassified by authorized personnel using appropriate procedures. I understand that U.S. classified information must be marked and protected according to AR 380-5, and that NATO material must be marked and protected according to AR 380-15.

c. Classified magnetic disks, compact disks, and other media will not be removed from the work area without the approval of the local commander or head of the organization.

d. If working in a classified area, I will ensure that only U.S. personnel with appropriate security clearances are allowed unescorted access to the systems.

e. If working in a classified area, I will ask my IASO about TEMPEST (Red/Black) separation requirements for system and network components, and I will ensure that those requirements are met.

f. I will use only approved methods to "air-gap" information to and from the SIPRNET.

9. I understand and will comply with the Public Key Infrastructure (PKI) requirements in AE Regulation 25-1-5 with regard to digitally signing and encrypting e-mail.

10. I will not attempt to defeat or bypass system or network security controls.

11. I know what constitutes a security incident or inadequate security and that I must immediately report such occurrences to my IASO.

12. I understand the information and requirements as presented in AE Pamphlet 25-25 and in this agreement, and will execute my responsibilities to keep my system and the network secure. If I am a supervisor, IMO, SA, or IASO, I will ensure that all users in my area of responsibility sign this agreement.

13. I know I am subject to disciplinary action if I violate DOD, Army, or Army in Europe computer security policy.

Computer-User Name	Security Officer Name
(Typed or Printed): _____	(Typed or Printed): _____
Computer-User Signature: _____	Security Officer Signature: _____
Date: _____	Date: _____